July 21, 2026

VIA EMAIL

The Honorable Brett Guthrie
Chairman
Energy & Commerce Committee
U.S. House of Representatives
Washington, DC 20515

The Honorable Frank Pallone
Ranking Member
Energy & Commerce Committee
U.S. House of Representatives
Washington, DC 20515

The Honorable Gus Bilirakis
Chairman
Subcommittee on Commerce,
Manufacturing, and Trade
U.S. House of Representatives
Washington, DC 20515

The Honorable Jan Schakowsky
Ranking Member
Subcommittee on Commerce,
Manufacturing, and Trade
U.S. House of Representatives
Washington, DC. 20515

Re: App Store Freedom Act, H.R. 3209

Dear Chairman Guthrie, Chairman Bilirakis, Ranking Member Pallone, and Ranking Member Schakowsky:

On behalf of the undersigned organizations, we write to convey concerns about H.R. 3209, the App Store Freedom Act (ASFA),[1] a bill that is slated to be a focus of the Subcommittee on Commerce, Manufacturing, and Trade hearing on *Legislative Proposals to Strengthen Consumer Protection in a Changing Marketplace* on July 22. We ask that this letter be included in the record for that hearing.

We are concerned that ASFA would introduce significant cybersecurity vulnerabilities and undermine user privacy that far outweigh the alleged benefits to competition that supporters claim will flow from forcing app stores to provide access to third-party apps and app stores. The effect would be most pronounced for youth. These concerns are not merely hypothetical. Indeed, the European Union (EU) has already imposed similar requirements on app stores under the Digital Markets Act (DMA). As we explain below, the results have been catastrophic for user security and privacy.[2]

As background, ASFA purports to improve "interoperability" between the Google and Apple app stores and any third-party app or app store. While interoperability as a general matter is a worthy goal, context matters. The major app stores provide multiple layers of protection to ensure that apps are free of known malware, protect personal data, and restrict access to problematic content such as overtly

[1] *App Store Freedom Act*, H.R. 3209, 119th Cong. (2025).
[2] Giuseppe Colangelo and Alba Ribera Martinez, Vertical interoperability in mobile ecosystems: Will the DMA deliver (what competition law could not)?, *International Review of Law and Economics* 83 (2025); Isabella Lorenzoni, Interoperability: U.S. and E.U. Perspectives Compared, George Washington Competition & Innovation Lab (2025).

pornographic apps. Requiring these platforms to provide equal access to third-party applications without safeguards to ensure that those third-party applications provide best-in-class security and privacy protections is an invitation to bad actors to take advantage of millions of unsuspecting users.

The EU provides a case study in what could go wrong were the United States to adopt legislation like the ASFA. App store interoperability requirements under the DMA have led to an increase in fraudulent banking apps, malware-infused apps, and pornographic apps.[3] While the U.S. app store ecosystem is not free of fraud and malfeasance,[4] in the EU, these bad practices have become more prevalent, and the DMA makes cracking down on harmful or illegal applications much more difficult.[5] By contrast, in the United States, in those instances where developers of applications that do not comport with app store policies had made it through the screening process, the companies behind the app stores were able to shut down the credentials of those developers and deny future access, as happened when a flood of "nudify" applications appeared in app stores.[6]

As in the EU, ASFA is likely to materially increase risks to cybersecurity and data privacy through its requirement that a company provide "access to any interface and hardware and software feature of the operating system."[7] Developers do this through application programming interfaces (APIs), which are used to ensure the smooth integration and interoperability of two applications. But APIs are also a major line of attack for actors trying to steal user data, especially without guardrails that would prevent unauthorized access to or misuse of personal information.[8] Indeed, ASFA requires no such guardrails. This is why some companies restrict access to sensitive APIs and require applications for use.[9]

Co-sponsors and supporters of ASFA have described the legislation as "a bill that will protect kids online."[10] The effect on America's youth would be the exact opposite, however, as evidenced by the EU's experiment with app store interoperability. Were the ASFA to become law, app store operators targeted

---

[3] *See, e.g.*, Heather West, Center for European Policy Analysis, *Europe's DMA: A Cybercriminal's Paradise?,* Center for Cybersecurity Policy and Law (Dec. 2025); Jim Kohlenberger, *When Interoperability Mandates Weaken Security - JIT Happens*, Trusted Future (Sept. 5, 2025); Suzanne Frey, A new layer of security for certified Android devices, *Android Developers Blog* (Aug. 25, 2025) ("recent analysis found over 50 times more malware from internet-sideloaded sources than on apps available through Google Play"); Stephen Nellis, Apple raises concern over first porn app on iPhone under EU rules, *Reuters* (Feb. 3, 2025); Jennifer Jacobs, Apple blasts EU over digital competition laws, warning they make 'fraud and scams' more likely, *CBS News* (Nov. 6, 2025); Centre for European Reform, Is The European Union Taking the Right Approach to App Fraud? (Nov. 12, 2024). *See also, e.g.*, ENISA, Threat Landscape: Finance Sector, January 2023 to June 2024 (2024), at Section 3.6 (describing "surge in mobile banking trojans" and "200% year-on-year growth in malware families targeting banking applications" following implementation of DMA); Kurt Knudson New Android malware can empty your bank account in seconds, *Fox News* (Nov 27, 2025) (addressing malware apps developed in EU exported to the U.S. market).

[4] Karen Garcia, Apple Store removes bogus app after California warns EBT recipients, *Los Angeles Times* (Sept. 19, 2025); E.U. presses Apple, Google and others to act against online scams, *Le Monde* (Sept. 23, 2025).

[5] *See supra*, note 3. *See also* Apple, Statement: The Digital Markets Act's impact on E.U. users (Sept. 24, 2025); European Union Agency for Cybersecurity (ENISA), Sectoral Threat Landscape. (Nov. 6, 2025), at Sections 2, 3, 4.2 and 6.1-6.3; ENISA, Identifying Emerging Cybersecurity Threats for 2030 (Mar. 2023), at Sections 3.2., 3.5, 3.7, and 3.10.

[6] Matt Burgess, Harmful 'Nudify' Websites Used Google, Apple, and Discord Sign-on Systems, *Wired* (Aug. 28, 2024).

[7] ASFA Sec. 2(2)(A).

[8] *See, e.g.*. United States Cybersecurity Institute, "What is an API? (Application Programming Interface" (Dec. 16, 2025); Akamai, "API Security Impact Study 2024 (Nov. 13, 2024); Akamai, Web Attacks up 33%, APIs Emerge as Primary Targets (Apr. 22, 2025); Cloudflare, Organizations Struggle to Identify and Manage Cybersecurity Risks of APIs (Jan. 9, 2024). *See also* Gibson et al.'s analysis of the 2021 LinkedIn Data Breach, "Vulnerability in the Massive API Scraping: 2021 LinkedIn Data Breach" (2021).

[9] *See, e.g.,* Apple, List of APIs that require declared reasons now available (Jul. 27, 2023).

[10] *See* Digital Progress Institute, et al., Letter to House Energy & Commerce Committee (Oct. 24, 2025); Reps. Lori Trahan and Kat Cammack, "Dear Colleague" Letter (Oct. 30, 2025).

by the legislation—Google and Apple—would have no ability to ensure the safety of apps, impose content restrictions on pornographic apps, or direct changes to third-party app stores or apps. Indeed, this legislation would prevent these platform operators from ensuring that parental controls actually work—despite those controls being the subject of extensive discussion during a previous hearing and the focus of at least two bills considered by the Subcommittee.[11] ASFA would both *weaken* protections that families rely on and *create new vulnerabilities* through third-party app stores.[12]

Sponsors of ASFA have also claimed that the legislation would foster the creation of a youth-friendly app store. It is worth noting that the Android operating system has allowed alternative app stores for years, and no such store exists. The same goes for Windows PCs and MacOS. There is nothing preventing a group of concerned developers from doing this today *without* the potentially catastrophic consequences for youth safety and privacy that would ensue from opening the floodgates to bad actors. Yet they have not done so. Policymakers, in other words, should not expect the sudden emergence of a youth-friendly app store if ASFA is enacted. Indeed, during a prior hearing, Chairman Guthrie suggested limiting the scope of ASFA to minor users—a proposal that would make sense if the intent of the legislation were to foster the development of a youth-focused app store. Yet the bill's supporters have not accepted that proposal because ASFA is not ultimately about youth safety—it is about increasing the bottom line of some of the world's largest app developers.[13]

Congress should take the EU's experience as a cautionary tale. The DMA has produced a fractured digital landscape marked by weaker protections, more harmful content, and increased risks to users. We strongly recommend against pursuing the regulatory approach taken by the EU, an approach which, according to the EU's own experts, has restricted the growth of its technology sector.[14] Were the United States to follow the EU approach, the risks to security, data privacy, and kids' safety would be severe. The United States has long warned against these outcomes. Instead of copying a regulatory model that has clearly failed, as ASFA does, Congress should prioritize policies that strengthen privacy, improve security, and support American innovation.

Thank you for your consideration of our views. We look forward to working with the Committee to advance legislation that protects the privacy and safety of youth online and promotes competition and innovation.

Respectfully submitted,

Software & Information Industry Association (SIIA)
Association for Competitive Technology (ACT)
Chamber of Progress
Computer & Communications Industry Association (CCIA)
NetChoice

---

[11] *Parents Over Platforms Act*, H.R. 6333, 119th Cong. (2025); *App Store Accountability Act*, H.R. 3149, 119th Cong. (2025).
[12] Aden Hizkias, The Hidden Risks of the App Store Freedom Act, Chamber of Progress (Nov. 5, 2025).
[13] *See, e.g.*, Eduardo Contreras, *Scandal-Plagued Companies Aren't Doing the Right Thing*, *D.C. Journal* (Apr. 16, 2024) (referencing ASFA predecessor legislation, the Open App Markets Act); X.com post by Adam Kovacevich (Dec. 12, 2025).
[14] Mario Draghi, *The Future of European Competitiveness* (Sept. 9, 2024); Enrico Letta, *Much More than a Market – Speed, Security, Solidarity: Empowering the Single Market to deliver a sustainable future and prosperity for all EU Citizens*, (Apr. 2024).